FSA Security Policy Matrix

🟩 Consistent with FSA Policy
🟨 Partially consistent with FSA Policy; Gaps exist
🟥 ED Policy and FSA Policy conflict

	SFA Guide	*ED Policy*	*Resolution Recommendation*
3.1 Personnel Security	Hiring, transfer, and termination procedures shall be established.		🟥 This policy is not addressed in Ed policy.
	Documented job descriptions that accurately reflect assigned duties and responsibilities and that segregated duties and sensitivity level shall be established.		🟥 This policy is not addressed in Ed policy.
	There shall be a documented process for requesting, establishing, issuing, and closing user accounts.		🟥 This policy is not addressed in Ed policy.
	A nondisclosure statement shall be required if individual needs access to privileged information.		🟥 This policy is not addressed in Ed policy.
	A submitted letter through contract representative shall be required for contractors to gain access to sensitive information.	Contractor personnel whose duties do not require a background investigation, but do require access to sensitive information will submit an access justification letter, and sign a Department non-disclosure agreement. (15)	🟩 No policy gap.
	When appropriate, terms and conditions of employment shall state that security responsibilities extend outside of the workplace (for example telecommuting, etc.)		🟥 This policy is not addressed in Ed policy.

3.1.1 Position Sensitivity Level	Positions shall be reviewed for sensitivity level or, if already employed by SFA, a planned date for completion of position sensitivity analysis shall be stated.	All contractor employees who develop or work on Department systems or information in any capacity will be properly evaluated for risk in accordance with the risk designation process as outlined in Handbook #11 and screened for trustworthiness as necessary. (14)	The policy only covers contractor positions, not all job positions.
3.1.2 Background Screening	Appropriate background screening for assigned positions shall be completed prior to granting access and reviewed periodically thereafter.	Contractor employees identified as requiring to undergo a security screening will not be allowed to work for on a Department contract or task order unless all necessary suitability request paperwork is provided to the appropriate Department official within 14 days of reporting for work. (14)	No policy gap.
	Every system shall describe conditions for allowing system access prior to completion of background screening and compensating controls to mitigate associated risk.	Contractor employees identified as requiring to undergo a security screening will not be allowed to work for on a Department contract or task order unless all necessary suitability request paperwork is provided to the appropriate Department official within 14 days of reporting for work. (14)	No policy gap.
3.1.3 Separation of Duties	Distinct and sensitive systems support functions shall be performed by different individuals to ensure that no individual has all necessary authority or information access which could result in fraudulent activity.	Where feasible, sensitive duties will be divided among multiple (separate) individuals to preclude any one individual, acting alone, from gaining the opportunity or capability to adversely affect the system. (16)	No policy gap.
	Whenever possible, development, test and operational facilities shall be separated to facilitate segregation of duties and prevent unwanted alteration and modification of operational systems.		This policy is not addressed in Ed policy.
3.1.4 Least Privilege	Formal policies shall be described that define the authority that will be granted to each user or class of users. User access shall be restricted to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform job.	Individuals will not be granted access to sensitive information beyond that required in job performance. (16)	Policies describing authority for each user level are not stated.

3.2 Physical and Environmental Protection	Adequate physical security controls shall be implemented that are commensurate with the risks of physical damage or access.	"Controlled areas" will be protected by physical security and other measures appropriate for the sensitivity or criticality of the area as determined by the results of a risk assessment. (17)	No policy gap.
	Secure areas shall have a clearly defined security perimeter, with appropriate barriers and access controls.		This policy is not addressed in Ed policy.
3.2.1 Supporting Utility Security	Electric power distribution, heating plants, water, sewage, and other supporting utilities shall be periodically reviewed for risk of failure.		This policy is not addressed in Ed policy.
3.2.1.1 Air Conditioning	Heating and air conditioning systems shall be regularly maintained.		This policy is not addressed in Ed policy.
3.2.1.2 Water	Plumbing lines shall be known and shall not endanger system, and plumbing leaks shall be addressed.		This policy is not addressed in Ed policy.
3.2.1.3 Power	An uninterruptible power supply or backup generator shall be provided.		This policy is not addressed in Ed policy.
3.2.2 Fire Control	Fire suppression and prevention devices shall be installed and working.		This policy is not addressed in Ed policy.

	Fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, shall be reviewed periodically.		This policy is not addressed in Ed policy.
3.2.3 Facilities	Access to facilities shall be controlled through the use of guards, identification badges, or entry devices such as keycards.		This policy is not addressed in Ed policy.
3.2.3.1 Visitors	Visitors, contractors, and maintenance personnel shall be authenticated through the use of preplanned appointments and identification checks, and shall also be escorted when in restricted or sensitive areas.		This policy is not addressed in Ed policy.
	Access to sensitive information shall be restricted to authorized personnel only.	Individuals will not be granted access to sensitive information beyond that required in job performance. (16)	No policy gap.
3.2.3.2 Access	Management and supervisors shall limit access to controlled areas based on valid need for access and shall also regularly review the list of persons with physical access to sensitive facilities.	Managers and supervisors will limit access to controlled areas and sensitive IT resources to only personnel who have a security screening commensurate with the sensitivity of the data accessed and have a valid need for access. (17)	No policy gap.

	Emergency exit and re-entry procedures shall ensure that only authorized personnel are allowed to re-enter after fire drills, etc.		This policy is not addressed in Ed policy.
	Unused keys or other entry devices shall be secured.		This policy is not addressed in Ed policy.
	Physical accesses shall be monitored through audit trails and apparent security violations shall be investigated and remedial action shall be taken.		This policy is not addressed in Ed policy.
	Controlled areas shall be determined by a risk assessment.	"Controlled areas" will be protected by physical security and other measures appropriate for the sensitivity or criticality of the area as determined by the results of a risk assessment. (17)	No policy gap.
	Access to telecommunications hardware or facilities shall be restricted and monitored.		This policy is not addressed in Ed policy.

3.2.3.3 Static Entry Codes	Access controls shall be addressed.		This policy is not addressed in Ed policy.
	Entry codes shall be changed periodically.		This policy is not addressed in Ed policy.
3.2.3.4 Suspicious Activities	Suspicious access activity shall be investigated and appropriate action shall be taken.		This policy is not addressed in Ed policy.
3.2.4 Data Intercept	Data shall be protected from interception. Physical access to data transmission lines shall be controlled and computer monitors shall be located to eliminate viewing by unauthorized persons.		This policy is not addressed in Ed policy.
3.2.5 Media Labeling and Logging	Deposits and withdrawals of tapes and other storage media from the library shall be authorized and logged.		This policy is not addressed in Ed policy.

	All media containing sensitive information shall display a sensitive information label.	Department personnel will ensure that sensitive materials are marked according to applicable regulations and guidance provided in Handbook #12. Appropriate marking and annotation are required for printed information, listings, diskettes and jackets, and storage devices. Appropriate preprinted labels, where possible, will be	No policy gap.
3.3 Production, Input/Output Controls			
3.3.1 Electronic Media Sanitation	Every system shall establish procedures for sanitizing electronic media for reuse and storing or destroying damaged/spoiled media.		This policy is not addressed in Ed policy.
3.3.2 User Support	Every system shall provide help desk or other user support that offers advice.		This policy is not addressed in Ed policy.
3.3.3 Hardcopy Destruction	Every system shall establish procedures for shredding or destroying hardcopy media when it is no longer needed. These procedures shall include some form of logging the destruction or other form of audit trail.	Procedures for destruction of media containing sensitive information are provided in Handbook 12.	This policy is not addressed in Ed policy.

	Controls shall be in place for transporting or mailing media or printed output.		This policy is not addressed in Ed policy.
3.3.4 Storage	Every system shall establish procedures and protection controls to ensure physical protection of media storage vault/library.	Media used to record and store sensitive software or information will be protected, controlled, and secured when not in actual use. (20)	This policy is not addressed in Ed policy.
3.3.5 Labeling	External labeling shall include special handling instructions.	Department personnel will ensure that sensitive materials are marked according to applicable regulations and guidance provided in Handbook #12. Appropriate marking and annotation are required for printed information, listings, diskettes and jackets, and storage devices. Appropriate preprinted labels, where possible, will be	No policy gap.
3.3.6 Access	Every system shall establish procedures to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information, and that only authorized users pick up, receive, or deliver input and output information and media.		This policy is not addressed in Ed policy.
	Authorization shall be required for the removal of all media from the organization, and an audit trail shall be maintained to record all such removals.		This policy is not addressed in Ed policy.

3.3.7 Logging	Every system shall maintain operator logs for all systems, including such entries as system start and finish times, system errors encountered and the corrective actions taken, batches run, etc. All entries shall be annotated by time and the operators name.		This policy is not addressed in Ed policy.
3.4 Contingency Planning/Disaster Recovery Plan	Every system shall describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable, and detailed plans shall be provided as an attachment.	Contingency planning is done by business managers to ensure that if mission essential or support IT systems and services are not available to support their business functions, the business process can continue to function and provide appropriate mission essential services even in a diminished capacity if	Section 3.13 does not cover all of the information required.
3.4.1 General Plans	A comprehensive plan shall be developed, documented, and tested prior to authorizing a system for processing.	System personnel will conduct a live Disaster Recovery test at least once during a certification cycle. (see the *Certification and Accreditation Guidance* document). (29)	No policy gap.
	The contingency plan shall be approved by key affected parties, in particular System Manager and the SSO, and distributed to all appropriate personnel.	System administration personnel and the SSO will review each disaster recovery plan and contingency plan. (29)	No policy gap.
	The plan shall be considered, at a minimum, sensitive, with access limited to a "need to know" basis, and shall be stored securely offsite.	DRPs and contingency plans will be considered sensitive, with access limited on a “need to know” basis. (30)	No policy gap.

	Every system shall assign responsibilities for recovery.		This policy is not addressed in Ed policy.
	Every system shall provide a copy of all DRPs and contingency plans to PO CSO.	Copies of all DRPs, contingency plans, and tests developed by each PO will be provided to the CSO and the DCIO/IA. (30)	No policy gap.
	Contingency planning shall incorporate the results of the latest Risk Assessment in order to focus attention on events that have the highest likelihood of disrupting service.		This policy is not addressed in Ed policy.
	Contingency plans and Disaster Recovery plans shall include the conditions necessary for activating the plan, including who is to be involved in the decision before each plan is activated.		This policy is not addressed in Ed policy.
	Every system shall include resumption procedures for returning to normal business operations in the plans.		This policy is not addressed in Ed policy.

3.4.1.1 Contingency Plan	Every system shall establish processing priorities and approved by management.		This policy is not addressed in Ed policy.
	Every system shall identify the most critical and sensitive operations and their supporting computer resources.		This policy is not addressed in Ed policy.
	Every system shall test contingency plans to permit continuity of mission-critical functions in the event of a catastrophic event.	Tests will be documented and the DAA and the DCIO/IA will be briefed on the results. (29)	No policy gap.
	Emergency procedures shall have required time-scales for recovery and restoration of specified services.		This policy is not addressed in Ed policy.
3.4.1.2 Disaster Recovery Plan	Every system shall document disaster recovery procedures.		This policy is not addressed in Ed policy.

3.4.1.3 Backup Plan	Every system shall backup procedures, including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup).	System operations personnel will ensure that appropriate backups are performed as directed by the business manager. (30)	This policy is the closest to the regulated policy.
	Every system shall determine a minimum level of backup information to ensure all essential business information and software can be recovered in case of media failure or a disaster. At least three generations/cycles of back-up information shall be retained for important applications.	Critical files (i.e., those containing security-related data and audit records and those designated critical by operational personnel) should be backed up nightly and stored in a secure container. (30)	There is no requirement for three generations/cycles of back-up information.
	System personnel shall ensure appropriate backups are performed as directed by the business manager.	System operations personnel will ensure that appropriate backups are performed as directed by the business manager. (30)	No policy gap.
	Every system shall stored backup tapes in a secure, off-site location; daily incremental backups shall be stored on-site; critical data files shall be backed up nightly.	Backup tapes shall be stored in a secure, off-site location; however, daily incremental backups may be stored on-site. (30)	No policy gap.
	System defaults shall be reset after being restored from a backup.		This policy is not addressed in Ed policy.

3.4.1.4 Emergency Plan	Every system shall document formal written emergency operating procedures.	All copies of DRPs and contingency plans will be maintained in a complete and current state ready for implementation at any time. Current copies also will be maintained at the primary site and the alternate site selected by each preparing organization. (30)	Policy does not require all system to have emergency operating procedures.
3.4.2 Testing	Every system shall document contingency/disaster recovery plans for all supporting IT systems and networks and plans , periodically tested, readjusted, and briefed to DAA.	This information is covered in section 3.13 Continuity of Operations Planning. (29)	No policy gap.
	Every system shall test contingency, disaster, and emergency plans biennially by system personnel.	System personnel will conduct a live Disaster Recovery test at least once during a certification cycle. (see the Certification and Accreditation Guidance document). (29)	Policy does not require biennial testing.
	Following each test, every system shall reassess and update contingency/disaster recovery plans to ensure its continued effectivity.	Any problems, omissions, or other deficiencies discovered during testing will be corrected and the appropriate portion of the plan retested until critical functions can be implemented within acceptable time frames. (30)	No policy gap.
3.4.2.1 Alternate Processing Site	The backup storage site and alternate site shall be geographically removed from the primary site and physically protected.	Backup tapes shall be stored in a secure, off-site location; however, daily incremental backups may be stored on-site. (30)	This policy is not addressed in Ed policy.

	If appropriate, every system shall use an alternate processing site with a contract or interagency agreement in place.		This policy is not addressed in Ed policy.
	Every system shall maintain the system/application documentation at an off-site location.		This policy is not addressed in Ed policy.
	Every system shall maintain detailed instructions for restoring operations.		This policy is not addressed in Ed policy.
3.5 Data Integrity	There shall not be unauthorized ability to enter maliciously, or accidentally alter, or destroy information.	Internal system controls will be implemented to prevent persons from either maliciously or accidentally altering or destroying information processed, stored, or transmitted by Department IT assets. (3)	No policy gap.
3.5.1 Virus Detection and Elimination	Every system shall install virus detection and elimination software. Once installed, every system shall have procedures for routinely updating virus signature files, automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on disk), and screening non-text files.	All Department-owned workstations and portable computing devices will have Department approved virus detection software installed. Updates to the virus definition tables will made readily available for download or be automatically "pushed" to each machine. (23)	No policy gap.

	Every system shall establish procedures to verify information regarding malicious software, and ensure that incoming warnings are accurate and not a hoax, including verification using reliable internet sites, reputable journals, etc.		This policy is not addressed in Ed policy.
	All information obtained from the Internet shall be considered suspect until confirmed by another source.		This policy is not addressed in Ed policy.
3.5.2 Reconciliation	Every system shall establish procedures to reconcile data, including a description of the actions taken to resolve any discrepancies.		This policy is not addressed in Ed policy.
3.5.3 Verification	Every system shall use integrity verification programs by applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing.		This policy is not addressed in Ed policy.
	Every system shall establish procedures for responding to validation errors.		This policy is not addressed in Ed policy.

	Every system shall incorporate validation checks that would detect corruption of correctly entered data by processing errors or deliberate acts. Additionally, every system shall validate output data to ensure the processing of correctly stored data is correct and appropriate.		This policy is not addressed in Ed policy.
3.5.4 Message Authentication	Every system shall use message authentication in the application to ensure that the sender of a message is known and that the message has not been altered during a transmission.		This policy is not addressed in Ed policy.
3.5.5 Performance Measurements	Every system shall use system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attacks and system and network slowdowns and crashes.		This policy is not addressed in Ed policy.
3.5.6 Intrusion Detection	Every system shall include a description of intrusion detection tools installed on the system, where they are placed, the type of processes detected/reported, and the procedures for handling instructions.		This policy is not addressed in Ed policy.
	Every system shall conduct periodic reviews on the software and data content of critical systems. All unapproved files or unauthorized amendments shall be formally investigated.		This policy is not addressed in Ed policy.

	Every system shall routinely review Intrusion detection reports and suspected incidents shall be handled accordingly.		This policy is not addressed in Ed policy.
3.5.7 Penetration Testing	Every system shall perform penetration testing on the system and every system shall establish procedures to ensure that they are conducted appropriately. Included in this section should be descriptions of the hardware and software, policies, standards, procedures, approvals related to automated information system security in the application/system on which it is processed, backup	All Web servers, both Internet and Intranet, will be certified and accredited before going 'live'. The servers will be certified and accredited in accordance with the *Certification and Accreditation Guide* , and the certification process will include penetration testing. (22)	ED policy does not give enough specific guidance for what needs to be included within penetration testing procedures.
3.6 Documentation	Every system shall maintain a System Security Plan.		This policy is not addressed in Ed policy.
	Every system shall maintain a list of documentation maintained for the application.		This policy is not addressed in Ed policy.

	Every system shall maintain a written agreement regarding how data is shared between interconnected systems (memoranda of understanding with interfacing systems).	IT systems or applications connected to the Department's network require a Memorandum of Agreement (MOA) between the system DAA (or application owner) and the Department DAA, which will provide assurances that appropriate security controls have been implemented. The MOA will be reviewed and validated by	No policy gap.
	Every system shall maintain application documentation, requirements, and specifications.		This policy is not addressed in Ed policy.
	Every system shall maintain software and hardware testing procedures and results.		This policy is not addressed in Ed policy.
	Every system shall maintain standard operating procedures that support all operations of the application or general support system.		This policy is not addressed in Ed policy.
	Every system shall maintain user manuals to explain how software/hardware is to be used.		This policy is not addressed in Ed policy.

	Every system shall maintain vendor-supplied vendor documentation of software and hardware.		This policy is not addressed in Ed policy.
	Every system shall maintain certification and accreditation documents and statements authorizing a system to process.	The Office of the DCIO/IA will serve as a central repository for all Department IT security related documents related to the Department's IT systems. All Principal Offices will provide the DCIO/IA with copies of all system level security plans, security reviews, corrective action plans, certification and accreditation packages	No policy gap, although SFA policy implies that the systems would maintain their own set of documentation..
	Every system shall maintain a list of support contacts in case of unexpected difficulties or system errors.		This policy is not addressed in Ed policy.
3.7 Configuration Management	Every system shall include a description on the hardware and system software maintenance controls in place or planned.		This policy is not addressed in Ed policy.

3.7.1 General	It shall be the responsibility of the CCB to provide an assessment of the security impact of each change or modification against security requirements and accreditation conditions issued by DAA.	Attendance of a security representative as a regular member of the CCB will ensure review of all proposed configuration changes for possible security implications. (28)	No policy gap.
	It shall be the responsibility of the CCB that the security representative attends CCB.	OCIO security personnel may be available to support PO CCBs upon request. (28)	No policy gap.
	It shall be the responsibility of the SSO to recommend approval of changes based on system security.	One of the steps for processing changes by the CCB will include a review by the responsible SSO, who will recommend approval or disapproval of the change based on the risk to the security of the system. (28)	No policy gap.
	CCB shall be formed within each PO to process, evaluate, and recommend approval or disapproval of proposed system configuration changes.	A Configuration Control Board (CCB) will be formed within each PO to process, evaluate, and recommend approval or disapproval of proposed system configuration changes.	No policy gap.
3.7.2 Configuration Control Board	Every system shall describe Configuration management procedures for the system.	This information is covered in section 3.12 Configuration Management.	No policy gap.

	A formal change control process shall be put in place for the system requiring that all changes to the application software are to be tested and approved before being put into production.		This policy is not addressed in Ed policy.
	Every system shall use software change requests forms to document requests and related approvals.		This policy is not addressed in Ed policy.
	Version control that allows association of system components to the appropriate system version shall be considered.		This policy is not addressed in Ed policy.
	Every system shall consider procedures for ensuring that contingency plans and other associated documentation are updated to reflect system changes.		This policy is not addressed in Ed policy.
	Every system shall use software distribution implementation orders including effective date provided to all locations.		This policy is not addressed in Ed policy.

	All new and revised hardware and software shall be authorized, tested, approved, and documented before distribution and implementation.		This policy is not addressed in Ed policy.
3.7.2.1 Change Management	Every system shall describe change identification, approval, and documentation procedures.	This information is covered in section 3.12 Configuration Management. (28)	No policy gap.
	An impact analysis shall be conducted to determine the effect of proposed changes on existing security controls, including the required training needed for both technical and user communities to implement the control.	The security impact of each change or modification to an information system or site configuration will be assessed against the security requirements and the accreditation conditions issued by the DAA. (29)	This policy does not address what training would be needed resulting from the change.
3.7.2.1.1 Documentation	All changes to application software shall be documented.		This policy is not addressed in Ed policy.
	Procedures for testing and/or approving system components (operating system, other system, utility, applications) shall be considered prior to promoting to production.		This policy is not addressed in Ed policy.

3.7.2.1.2 Testing	The type of test data to be used (live or made-up) shall be specified.		This policy is not addressed in Ed policy.
	Test results shall be documented.		This policy is not addressed in Ed policy.
	Detailed system specifications shall be prepared and reviewed by management.		This policy is not addressed in Ed policy.
3.7.2.1.3 Approval	Special procedures for performance of emergency repair and maintenance shall be considered.		This policy is not addressed in Ed policy.
3.7.2.1.4 Emergency Changes	Emergency change procedures and how the emergency fixes are handled/to be handled shall be documented and approved by management, either prior to the change or after the fact.		This policy is not addressed in Ed policy.

3.7.3 Procedures and Guidance	Every system shall describe restrictions/controls on those who perform maintenance and repair activities, both on-site and off-site (i.e., escort of maintenance personnel, sanitization of devices removed from the site, etc.).	Contract maintenance personnel and others not authorized for unrestricted access to a controlled area but are required to perform work in a controlled area will be escorted by authorized persons at all times while in a controlled area. (17)	This policy is not addressed in Ed policy.
3.7.3.1 Maintenance and Repair	All vendor-supplied default security parameters shall be reinitialized to more secure/most restrictive settings.		This policy is not addressed in Ed policy.
	Every system shall describe procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.		This policy is not addressed in Ed policy.
	Implementation of changes shall take place at such times and in such a way as to limit disturbing the business process involved.		This policy is not addressed in Ed policy.
3.7.3.2 Illegal Software	Whatever is not expressly allowed is denied.		This policy is not addressed in Ed policy.

	There shall be organizational policies for handling and protecting against illegal use of copyrighted software or shareware, and the use of copyrighted software, shareware, and personally owned software/equipment shall be documented.	· No privately owned software or utilities will be used on the Department's computers without specific authorization from the DCIO/IA or his or her designate. · Requests for authorization to use privately owned software will be made in writing through the employee's supervisor or manager and CSO. Each request must	No policy gap.
	Periodic audits shall be conducted of users' computers to ensure that only legally licensed copies of software are installed.		This policy is not addressed in Ed policy.
	Procedures shall contain provisions for individual and management responsibilities and accountability, including penalties.		This policy is not addressed in Ed policy.
	If a copyrighted commercial off-the-shelf product/shareware is used, sufficient licensed copies of the software shall be purchased for all of the systems on which this application will be processed.		This policy is not addressed in Ed policy.
3.7.3.3 Application Licensing	Hardware/software warranties shall be managed to minimize the cost of upgrades and cost-reimbursements or replacement for deficiencies.		This policy is not addressed in Ed policy.

	It shall be stated whether the government owns the software, if the software was developed in-house or under contract, or if the application software was received from another federal agency with the understanding that it was federal government property.		This policy is not addressed in Ed policy.
3.8 Incident Response Capability			
3.8.1 General	Intrusions detection tools, automated audit logs, penetration testing, and other preventative measures shall be employed to provide help to users when a security incident occurs in the system.		This policy is not addressed in Ed policy.
3.8.2 Preventative Measures	Privately owned software or utilities shall not be used on Departmental computers without specific authorization.	No privately owned software or utilities will be used on the Department’s computers without specific authorization from the DCIO/IA or his or her designate. (32)	No policy gap.
	Media shall be free of all viruses before being used with Department's computers .	The CSO shall ensure that media are free of viruses and other malicious software before authorizing their use. (33)	No policy gap.

	Procedures shall be in place for recognizing, handling, and reporting incidents.	Specific incident reporting and response procedures are found in the *Incident Reporting and Response Guide* . (32)	No policy gap.
3.8.3 Incident Identification and Resolution	Incidents shall be monitored and tracked until resolved.		This policy is not addressed in Ed policy.
3.8.3.1 Incident Identification	Security alerts and security incidents shall be analyzed and remedial actions shall be taken.		This policy is not addressed in Ed policy.
	Users are required to notify any observed or suspected security weaknesses in, or threats to, the organizations systems or services to management and/or system administrators as soon as possible. They should not attempt to prove a suspected weakness on their own.	All Department and contractor employees are responsible for helping to ensure the security of Department IT systems and information. Part of this responsibility is to report any confirmed or suspected security events or incident in a timely manner. (31)	No policy gap.
	Software malfunctions shall be reported and handled.	This information is included in section 3.15 Incident Reporting and Response. (31)	No policy gap.

3.8.3.2 Post Incident	Incident handling procedures and control techniques shall be modified after an incident occurs.		This policy is not addressed in Ed policy.
	Audit trails and other evidence shall be collected and secured for analysis and as potential evidence.		This policy is not addressed in Ed policy.
	Incidents shall be reported to FedCIRC, NIPC, and local law enforcement when necessary.		This policy is not addressed in Ed policy.
3.8.4 Information Sharing	Incident information and common vulnerabilities or threats shall be shared with interconnected systems.		This policy is not addressed in Ed policy.
	SFA Management shall assign specific individual(s) to receive and respond to alerts/advisories, vendor patches, exploited vulnerabilities, etc.		This policy is not addressed in Ed policy.

FSA Security Policy Matrix

🟩 Consistent with FSA Policy
🟨 Partially consistent with FSA Policy; Gaps exist
🟥 ED Policy and FSA Policy conflict

2.1 Risk Management			
	SFA Guide	***ED Policy***	***Resolution Recommendation***
4.1 Identification and Authentication	Each system user shall be uniquely identified and verified by the system before being granted access.	It is the policy of the Department that ***each system user shall be uniquely identified (identification) and verified (authentication) by the system before being granted access*** . (23)	🟩 No policy gap.
	Every system shall describe the passwords, tokens, biometrics, and other methods used to identify and authenticate.	Positive I&A of authorized users of remote processing facilities will be made through the use of effective I&A systems (passwords, biometrics). (23)	🟨 Policy by ED does not provide specific detail for authentication methods.
	Every system shall describe how the application identifies access to the system.		🟥 This topic is not addressed in ED policy.
	Security controls shall be able to detect unauthorized access attempts.	The system will record at a minimum the following types of events: successful and unsuccessful log-in attempts, etc. (25)	🟨 Policy does not specifically include "unauthorized access attempts."
	Passwords shall be transmitted and stored with one-way encryption.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	🟨 Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	Vendor-supplied/default passwords shall be replaced immediately.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	🟨 Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	Passwords shall not be displayed when entered.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	🟨 Policy in Publication 112 may or may not have information specifically pertaining to the topic.

	Every system shall describe the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port), and the actions taken when that limit is exceeded shall be included.	The system will record at a minimum the following types of events: successful and unsuccessful log-in attempts. (25)	The policy does not describe actions taken when invalid access attempts exceed the set limit.
	Every system shall describe the self-protection techniques for user authentication mechanism.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	This topic is not addressed in ED policy.
	Log in procedures shall limit the amount of information about the system until after a successful log-in has occurred. This shall include: not displaying system or application identifiers until after a successful log-in; not providing help messages during the log-on procedure that would assist an unauthorized user; not validating any portion of the log-in information until all components have been completed, and not indicating which part of the log-in data was incorrect.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	This topic is not addressed in ED policy.
4.1.1 General Policy	Procedures shall be in place for handling lost and compromised passwords.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented.	Policy in Publication 112 may or may not have information specifically pertaining to the topic.

	Passwords shall be distributed securely and users shall be informed not to reveal their passwords to anyone (social engineering).	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented.	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	User ID and password shall be changed in the event of employee transfer, termination, retirement, or suspicion that the password has been disclosed.	Situations that require the deactivation of a user ID or the changing of a password: The transfer, termination, retirement, resignation, or reassignment of a Department IT system user. The suspicion or knowledge that a password has been disclosed to unauthorized parties. (24)	No policy gap.
	Before access is granted, the following shall be checked: the user has authorization from the system owner to access the system; the level of access is appropriate for the user's business purpose; segregation of duties has not been compromised; the user has been provided a copy of the Rules of Behavior for the system and has signed a statement indicating that they understand and agree to the Rules.	Individuals will not be granted access to sensitive information beyond that required in job performance. (16)	This topic is not addressed in ED policy.

	Any systems' privileges (any features allowing a user to override system or application control) shall be identified and associated with the categories of staff that would use them. An authorization process and record of privileges that may be allocated shall be maintained, and the process shall be completed before any privileges are granted.		This topic is not addressed in ED policy.
4.1.2 Identification Accountability	The system shall correlate actions to users via the creation of unique user IDs for each individual user. Group IDs shall be permitted only necessary.		This topic is not addressed in ED policy.
	Privileges (any features allowing a user to override system or application control) shall be assigned to a different user ID than that used for normal business use.		This topic is not addressed in ED policy.
	User IDs shall not give indication of the user's privilege level.		This topic is not addressed in ED policy.
	Every system shall describe how the access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).		This topic is not addressed in ED policy.

	Guest accounts are not allowed on EDNet.	***Except for Internet public access, guest or "anonymous" accounts on EDNet will not be allowed. Further, guest or anonymous accounts for any Department AIS are not to be used for any production or live system or network.*** (19)	No policy gap.
4.1.3 Host Based Identification	If host-based authentication is used, it shall be indicated. (This is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access.)		This topic is not addressed in ED policy.
4.1.4 Biometrics	Every system shall describe any biometrics and token controls that are used and how they are implemented on the system. (Indicate if special hardware readers are required, if users are required to use a unique PIN, who selects the pin, etc.)		This topic is not addressed in ED policy.
4.1.5 Public Key Infrastructure	Every system shall describe how digital signatures or electronic signatures will be used.	Two important applications of cryptography are digital signatures and encryption. Determining that information was not altered after it was signed provides message integrity and non repudiation. Encryption can help keep information and communications confidential. Each of these security tools will be considered when designing Department IT systems to conduct electronic commerce. (19-20)	No policy gap.

4.1.5 Public Key Infrastructure	PKI technology shall conform with FIPS 186-1, Digital Signature Standard and FIPS 180-1, Secure Hash Standard issued by NIST, unless a waiver has been granted. If a waiver has been granted, the name and title of the official granting the waiver shall be included.		This topic is not addressed in ED policy.
	Every system shall describe cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.		This topic is not addressed in ED policy.
4.1.6 Passwords			
4.1.6.1 Frequency of Change	Passwords shall be changed at least every ninety days or earlier if needed. Every system shall describe how password changes are enforced and who changes the passwords.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	If users will maintain their own password, it shall be ensured that they are provided with an initial secure password that they will be forced to change immediately.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.

	Temporary passwords (for use when a user forgets their password) shall only be given after first positively identifying the user. The temporary password shall only be given to users in a secure method, and shall require the user to change it immediately.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
4.1.6.2 Format	Passwords shall be a minimum of six to eight characters in a combination of alpha, numeric, upper/lower case or special characters, and shall meet FIPS Publication 112 standards.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	Password policy shall be documented, including the specific information on allowable character set, password length (maximums and minimums), password aging time frames and enforcement approach, and number of generations of expired passwords disallowed for use.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
4.1.6.2.1 Compliance	Procedures shall be put in place to determine compliance with password policies.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
	Password crackers/checkers shall be used.	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.

4.1.6.3 Scripts with Passwords	Every system shall describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are allowed only for batch applications).	Standards contained in Federal Information Processing Standards (FIPS) Publication 112, *Password Usage,* are the minimum standards for the Department and will be fully implemented. (23)	Policy in Publication 112 may or may not have information specifically pertaining to the topic.
4.1.7 Bypassing Controls	Every system shall describe policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.		This topic is not addressed in ED policy.
	Every system shall determine whether emergency or temporary access is authorized.		This topic is not addressed in ED policy.
4.1.8 Access Control Lists	A current list of authorized users and their access shall be created, maintained, and approved. This access control list shall be encrypted and meet federal standards.		This topic is not addressed in ED policy.

	It shall be indicated how often Access Control Lists are reviewed (at least every six months) to identify and remove users who have left the organization (inactive users), users whose duties no longer require access to the application, or redundant user IDs and accounts.		This topic is not addressed in ED policy.
	Authorization for privileged access rights shall be reviewed at least every three months to check if privileges should still be provided, and that no unauthorized privileges have been obtained.		This topic is not addressed in ED policy.
	Access to network services shall be controlled to the granularity of an individual user.	Access control will be capable of including or excluding access down to the level of a single user. (24)	No policy gap.
4.2 Logical Access Controls	Logical access controls are the system-based mechanisms used to specify who or what is to have access to a specific system resource and the type of access that is permitted.		This topic is not addressed in ED policy.
4.2.1 General	Every system shall describe the controls in place to authorize or restrict the activities of users and system personnel within the application.	Access control mechanisms will be used to restrict the access of users, processes, and other external entities (including non-IT system users) to sensitive information, functions, and services. (24)	No policy gap.

4.2.1 General	Every system shall describe hardware or software features that are designed to permit only authorized access to or within the application.		This topic is not addressed in ED policy.
	Trust relationships among hosts and external entities shall be appropriately restricted.		This topic is not addressed in ED policy.
	Access controls shall reside at the network, operating system, and application level to restrict users to the level of information to which they are authorized to gain access.		This topic is not addressed in ED policy.
4.2.2 Application	Every system shall indicate if the security software allows application owners to restrict the access rights of other application users, the general support system administrator, or operators to the application programs, data, or files.		This topic is not addressed in ED policy.
	Access to all program libraries, system software, and system hardware shall be restricted and controlled.		This topic is not addressed in ED policy.
	Privileges (any features allowing a user to override system or application control) shall be allocated to individuals on a need-to-use or event-by-event basis, i.e. per the minimum required for their job and only when needed.		This topic is not addressed in ED policy.

	Every system shall describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users.		This topic is not addressed in ED policy.
	Logical access controls shall restrict users to authorized transactions and functions.		This topic is not addressed in ED policy.
	Every system shall describe restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.		This topic is not addressed in ED policy.
	Access to security software shall be restricted to security administrators.		This topic is not addressed in ED policy.
	Inactive terminals in high-risk locations shall shut down after a defined period of inactivity, closing all applications, clearing the terminal screen, and closing the network session.		This topic is not addressed in ED policy.
4.2.3 Files	Internal security labels shall be used to control access to specific information types or files, and shall specify protective measures. Additional handling instructions shall be indicated.	Department personnel will ensure that sensitive materials are marked according to applicable regulations and guidance provided in Handbook #12. Appropriate marking and annotation are required for printed information, listings, diskettes and jackets, and storage devices. Appropriate preprinted labels, where possible, will be used for standardization. All media containing sensitive information must display the message *"Contains Sensitive Information"* externally in a clear and recognizable format. (17)	No policy gap.
4.2.3 Files	Access shall be restricted to files at the logical view or field.		This topic is not addressed in ED policy.
	Files shall not be downloaded to a network or shared drive.		This topic is not addressed in ED policy.

4.2.4 Delegate Permission	Every system shall describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users.	The enforcement mechanism (e.g., self/group/public controls, access control lists) will allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or both. Only the owner of an object will grant access to that object to other authorized users. (24)	No policy gap.
	Only the object owner shall grant access to an individual user or specified user group.	Access to specific information, files or documents residing anywhere on the network will require written authorization by the owner of the information. (20)	No policy gap.
4.2.5 Desktop	Users shall disable Java.	The standard workstation software load installed by OCIO will contain a network browser with Java disabled. (20)	No policy gap.
4.2.5 Desktop	Terminals shall automatically log off and screensavers shall lock the system after a period of inactivity.		This topic is not addressed in ED policy.
	Network connections shall automatically disconnect at the end of a session.	Appropriate controls will be implemented to preclude communication ports from remaining open and attached to a processor following either normal or abnormal termination of the communication link. (20)	No policy gap.
4.2.6 Firewall and Proxy	If the public accesses the system, controls shall be in place and implemented to protect the integrity of the application and the confidence of the public.	Each publicly accessible Web site will provide a Department approved privacy and security notice to all users that access the Web sites. (22)	The policy only lists one control related to protecting the public's information.
	Every system shall describe any type of secure gateway or firewall in use, including its configuration (e.g., configured to restrict access to critical system resources and to disallow certain types of traffic to pass through to the system).		This topic is not addressed in ED policy.

	Insecure protocols (UDP, ftp, etc) shall be disabled, unless specifically required by the system and prior authorization is granted.		This topic is not addressed in ED policy.
	Internet services leaving or entering a departmental IT system will be controlled via firewall or proxy devices.	***Internet services leaving or entering a Department IT system will be controlled via firewall or proxy devices*** . (18)	No policy gap.
	Information shall be provided regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.		This topic is not addressed in ED policy.
4.2.7 Encryption	Every system shall describe cryptography, specifically digital signatures and encryption.	Cryptographic technologies are an essential tool for security and trust in electronic systems, including EC. Two important applications of cryptography are digital signatures and encryption. Determining that information was not altered after it was signed provides message integrity and non repudiation. Encryption can help keep information and communications confidential. Each of these security tools will be considered when designing Department IT systems to conduct electronic commerce. (19)	No policy gap.
	All sensitive information shall be encrypted before being sent over the Internet.	Transmission of information over the Internet that is Department sensitive, government proprietary, or covered by the Privacy Act must follow the Department's encryption policy. (21)	No policy gap.
	Unencrypted Departmental material cannot be posted to a publicly accessible Internet site without prior approval.	Users will not post Department records (e.g., software, internal memos, internal policies, Department information and data) on any publicly accessible Internet site unless the posting is approved in writing by the DCIO/IA, or appropriate senior level Department official.	No policy gap.

4.2.7 Encryption	Every system shall describe procedures for key generation, distribution, storage, use, destruction, and archiving, and encryption shall meet federal standards.		This topic is not addressed in ED policy.
	In addition to securely managing secret and private keys, public keys shall be protected to prevent forging a digital signature by replacing the public key. Public keys shall be protected using public key certificates. There shall be procedures detailing how the certificates are generated and controlled.		This topic is not addressed in ED policy.
4.2.8 Network	Every system shall describe whether encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. If encryption is used primarily for authentication, include this information in that section.	All classified and sensitive information that is processed, stored and transmitted will follow the procedures defined in the Department's encryption policy. (26)	The Department encryption policy is never specifically addressed.
	There shall be logical controls for telecommunication access.	This information is covered in sections 3.8 Communications Security, 3.9 E-mail/Voice Mail Security, and 3.10 Facsimile Security. (26)	No policy gap.
	All unused network services shall be deactivated.	As a general policy, all unnecessary and unused network services will be removed from all network servers, routers and switches. (19)	No policy gap.
	IP addresses shall not be published.	These protective features will perform security functions (e.g., shielding the Internet Protocol [IP] address of the client on the base network) while still allowing clients on the network to access the external host. (18)	No policy gap.

	Every system shall describe network diagrams and documentation on setups of routers and switches.		This topic is not addressed in ED policy.
	Communication software shall be implemented to restrict access through specific terminals.		This topic is not addressed in ED policy.
	Devices that provide access mediation services shall include facilities to enforce access control.	Devices that provide access mediation services (e.g., router, firewall, bastion host) will themselves include facilities to enforce access control. (19)	No policy gap.
	Authorization procedures shall determine which network and network services are allowed to be accessed, and who gets to access them.	Access control mechanisms will be used to restrict the access of users, processes, and other external entities (including non-IT system users) to sensitive information, functions, and services. (24)	The policy does not specifically state "network and network services."
	It shall be determined whether networks should use enforced paths to restrict routes used between user terminals and the computer services that the user is authorized to use.		This topic is not addressed in ED policy.
4.2.9 System Interconnection	Security controls of the system and interconnected systems shall be reviewed.		This topic is not addressed in ED policy.
	A list of interconnected systems (including Internet), their names/unique identifiers, and a description of the interaction(s) among systems shall be included.		This topic is not addressed in ED policy.
	Every system shall describe the sensitivity level of each system.	Owners of *data* will be responsible for determining sensitivity of the *information* needed to support their functions and specifying the appropriate protection requirements. (35)	No policy gap.

	Every system shall describe the System of Record, if applicable.		This topic is not addressed in ED policy.
	Every system shall describe the name and title of authorizing management officials and the date of authorization.		This topic is not addressed in ED policy.
	Every system shall discuss security concerns and considerations, and the Rules of Behavior of the other systems that need to be considered in the protection of the system, including organizations owning the other systems.		This topic is not addressed in ED policy.
	Every system shall determine whether the software resides on an open network used by the general public or with overseas access.		This topic is not addressed in ED policy.
	If the application is running on a system that is connected to the Internet or other WANs, additional hardware or technical controls shall be installed and implemented to provide protection against unauthorized system penetration.	Multiple policies are included in section 3.4.8, including: · Web servers will be hosted within either a demilitarized zone (DMZ) or a separately protected zone behind a firewall, and the server operating system and applications software will be protected with access controls. (22)	This topic is not addressed in ED policy.

4.2.10 Fraud Waste and Abuse	The use of government equipment and software utilities for anything other than government-approved purposes is prohibited.	Further examples of prohibited activities considered abuse of Department computer assets include the following: Using E-mail for other than government-approved purposes. Using Department computer resources for personal gain. Using Department computer resources to play computer games at any time. Unauthorized access to manipulate official information Use of the Department network or systems for unapproved connectivity to any external system. Inappropriate Use of the Internet. (35)	No policy gap.
4.2.11 Web Policy	The CIO is responsible for maintenance and security of all Web servers.	Senior officials of each PO will ensure security measures will be documented and implemented to protect the hardware and the application and operating system software of their PO sponsored web-sites, web pages and web services. (21-22)	CIO is not specifically identified as responsible senior official.
	The SSO is responsible for all servers and security services for each Web server.	Each PO operating a Department Web site will assign an SSO to implement technical security "best practices" with regard to its establishment, maintenance, audit, and administration. (21)	The SSO is not specifically assigned the responsibility of Web servers.
	Web servers shall be hosted behind a firewall and Web services shall have appropriate access control.	Web servers will be hosted within either a demilitarized zone (DMZ) or a separately protected zone behind a firewall, and the server operating system and applications software will be protected with access controls. (22)	No policy gap.
	Web services shall be accredited, including penetration testing. Refer to C&A.	All Web servers, both Internet and Intranet, will be certified and accredited before going 'live'. The servers will be certified and accredited in accordance with the *Certification and Accreditation Guide* , and the certification process will include penetration testing. (22)	No policy gap.
	Disaster recovery plans and contingency plans shall be developed for each website. Refer to Contingency Plan.	Each Web-site will have a security plan, including a disaster recovery and contingency plan. (22)	No policy gap.
	Measures shall be in place to detect unauthorized access to Web servers and services.	Before final accreditation occurs, procedures and mechanisms will be established to ensure prompt detection of unauthorized access or modification to Web servers and services. (22)	No policy gap.

	All users shall be authenticated at the firewall when they connect to Department internal computers via the Internet.		This topic is not addressed in ED policy.
	Each Web page shall have a designated author or maintainer.		This topic is not addressed in ED policy.
	All publicly writeable directories will be reviewed and cleared each evening.		This topic is not addressed in ED policy.
4.2.11.1 Web Site Privacy Policy	Each publicly accessible Web site shall provide a privacy and security notice to users upon initial access.	Each publicly accessible Web site will provide a Department approved privacy and security notice to all users that access the Web sites. (22)	No policy gap.
	Information protected by the Privacy Act shall not be posted on publicly accessible Web servers.		This topic is not addressed in ED policy.
4.2.12 Warning Banners	A DOJ approved standardized log-on banners shall be placed on the system to warn unauthorized users that they have accessed a U.S. government system and can be punished.	All Department network components, internet web sites and applications, and Department IT systems will display a warning notice as part of the "greeting" BEFORE user login. The warning notice will include an "Authorized Use Only" warning and note that prosecution may arise from unauthorized use. (18)	The policy does not require that the log-on banner include the notification that it is a government system.

	All department networks shall display a warning notice before user login to include: Authorized Use Only warning, Consent to Monitoring notice, not identify the type of computers, network, or operating system.	***All Department network components, internet web sites and applications, and Department IT systems will display a warning notice as part of the "greeting" BEFORE user login*** . The warning notice will include an "Authorized Use Only" warning and note that prosecution may arise from unauthorized use. Include a "Consent to Monitoring" notice. Networks will implement positive user acknowledgment of consent to monitoring - such as having the user click a button or type 'yes', before admittance into the network. Not identify the type of computers, network, or operating system utilized on the network and not use words such as "Welcome." (18)	No policy gap.
4.2.13 Remote Access	Dial-in access shall be monitored.	Remote access via dial-in modem will be audited. (18)	No policy gap.
4.2.13 Remote Access	Approval by the system's manager is required for dial-in security. The SSO should review users requests for dial-in access.		This topic is not addressed in ED policy.
	Controls shall be put in place to allow users to access the system remotely. Remote access via dial-in modem will be an auditable event.	The following policies will apply to remote access to Department IT assets via dial-up modems: In addition to the user ID and password needed for normal Department IT access, a second means of secure authentication will be required. Authentication mechanisms or schemes such as using a password-protected modem, callback, encryption, or software that generates a one-time password will be considered. Remote access via dial-in modem will be audited. (20)	No policy gap.

	Additional security beyond user ID and password shall be incorporated into the dial-up policy.	The following policies will apply to remote access to Department IT assets via dial-up modems: In addition to the user ID and password needed for normal Department IT access, a second means of secure authentication will be required. Authentication mechanisms or schemes such as using a password-protected modem, callback, encryption, or software that generates a one-time password will be considered. (20)	No policy gap.
	Remote access to diagnostic ports shall be securely controlled.		This topic is not addressed in ED policy.
4.3 Audit Trails			
4.3.1 Review	Audit trails shall be reviewed frequently and according to strict guidelines.	Audit records shall be reviewed on a periodic basis, not less than weekly, to detect anomalies and ensure timely investigation. (25)	No policy gap.
4.3.1 Review	Audit trails shall be used as online tools to help identify problems other than intrusions as they occur.		This topic is not addressed in ED policy.
	Access to online audit logs shall be strictly controlled. Controls shall be in place to protect against unauthorized changes and operational problems.	Each system will create and maintain a “read only” audit trail of sensitive events that will be protected from modification or unauthorized access or destruction. Audit records shall be protected so that access is limited to the CSO, the SSO, and other authorized individuals. (25)	The policy does not specifically address online audits.
	Automated tools shall be used to review audit records in real time or near real time.		This topic is not addressed in ED policy.
	Appropriate system-level or application-level administrator shall review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.		This topic is not addressed in ED policy.

	The organization shall use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data.		This topic is not addressed in ED policy.
4.3.2 Content	All activity involving access to and modification of sensitive or critical files shall be logged.		This topic is not addressed in ED policy.
	Audit trails shall provide accountability by providing a trace of user actions.	For each recorded event, the audit record will identify the date and time of the event, user, type of event, and its success or failure. The SSO will be able to selectively audit the actions of any user(s) based on individual identity.(25)	No policy gap.
	Audit trails shall support after-the-fact investigations of how, when, and why normal operations ceased.	The audit trail will be sufficiently detailed to reconstruct events and aid in determining the cause or magnitude of compromise should a security incident or violation or malfunction occur. (25)	No policy gap.
	Audit trail shall have capability of being queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.	For each recorded event, the audit record will identify the date and time of the event, user, type of event, and its success or failure. (25)	The policy is not sufficient to meet the requirement.

	Audit trails shall include sufficient information to establish what events occurred and who (or what) caused them. In general, an event record shall specify: Type of event; When the event occurred; User ID associated with the event; and Program or command used to initiate the event.	For each recorded event, the audit record will identify the date and time of the event, user, type of event, and its success or failure. (25)	The policy does not include a requirement for logging information about the program used to initiate the event.
	Audit trails shall provide record of the number of successful and rejected system access attempts, data access attempts, and other resource access attempts.	The system will record at a minimum the following types of events: successful and unsuccessful log-in attempts, deletions of objects, and any attempts to modify or delete audit data. (25)	The policy does not include a requirement for including data access attempts monitoring.
	Audit trails shall be designed and implemented to record appropriate information that can assist in intrusion detection.	The audit trail will be sufficiently detailed to reconstruct events and aid in determining the cause or magnitude of compromise should a security incident or violation or malfunction occur. (25)	No policy gap.
	Audit trail clocks shall be kept synchronized to an agreed upon standard to avoid discrediting the validity of the logs during an investigation. Procedures shall be in place to check and correct any deviations in the time.		This topic is not addressed in ED policy.
4.3.3 Access Control	The confidentiality of audit trail information shall be protected if, for example, it records personal information about users.	Audit records shall be protected so that access is limited to the CSO, the SSO, and other authorized individuals. (25)	Policy is vague about protecting confidentiality.

	If off-line storage of audit logs are retained for a period of time, access to audit logs shall be strictly controlled.	Audit records shall be stored and accessible for a minimum of one year. (25)	The policy does not address how logs will be controlled.
4.3.4 Keystroke Monitoring	Whenever keystroke monitoring is used, reference to the policy and the means of notification shall be provided. Also indication of whether the DOJ has reviewed the policy shall also be provided		This topic is not addressed in ED policy.
4.3.5 Separation of Duties	There shall be a separation of duties between security personnel who administer the access control function and those who administer the audit trail.		This topic is not addressed in ED policy.